IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

TCYK, LLC,	)	
	)	
Plaintiff,	)	
	)	No. 13 C 3845
v.	)	
	)	
DOES 1–87,	)	Judge John J. Tharp, Jr.
	)	
Defendants.	)	

MEMORANDUM OPINION AND ORDER

Plaintiff TCYK, LLC, brings a complaint for copyright infringement against eighty-seven unnamed "John Doe" defendants[1] who, it alleges, unlawfully acquired and transferred the plaintiff's copyrighted motion picture, "The Company You Keep" (the "Movie"). The Court previously granted the plaintiff leave to subpoena the nonparty Internet Service Providers (the "ISPs") from which the Doe defendants obtain Internet access in order to discover the Doe defendants' true identities, prohibiting the plaintiff from publishing the identities of the Doe defendants in any way without the Court's leave. Now before the Court are three motions by three defendants that seek to quash the subpoenas, sever and dismiss the defendants, and impose a protective order. For the reasons that follow, the motions are denied.

BACKGROUND

The Doe defendants are currently known to the plaintiff only by the Internet Protocol ("IP") addresses assigned to them by their ISPs. The plaintiff issued third-party subpoenas to the ISPs requesting information sufficient to identify the true identity of each of the Doe defendants.

[1] The plaintiff has voluntarily dismissed eight of the eighty-seven Doe defendants. *See* Dkts. 21, 23. None of the dismissed defendants filed any of the motions under consideration here.

Some of those defendants, after being notified of the subpoena by their ISP, have moved to quash the subpoenas or to sever and dismiss the Doe defendants as improperly joined. The following motions are before the Court:

- John Doe No. 74, IP address 98.212.180.132, moves to quash the subpoena and for a protective order on the grounds that the subpoena violates his or her privacy, is overbroad, would not lead to relevant or admissible information, and does not suitably verify the basis of the request. Doe No. 74 additionally argues that it would violate his or her due process rights to be subject to discovery without having first been served with a complaint. Dkt. 16.

- Ashley Sierra, on behalf of IP address 71.239.76.10, moves to quash the subpoena because it violates Illinois Supreme Court Rule 224, which governs certain discovery procedures in Illinois state courts, and the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. §§ 2701–2703, which prohibits disclosure of the contents of electronic communications except in some circumstances. Dkt. 18.

- John Doe No. 22, IP address 76.16.62.222, moves to sever and dismiss Does 2–87 because joinder is improper under the Federal Rules of Civil Procedure. Dkt. 19.

DISCUSSION

The arguments asserted in these motions have been examined at length in other opinions issued by courts in this district and elsewhere. This Court's discussion is therefore brief.

I. The BitTorrent Protocol

The plaintiff alleges that each of the defendants used the BitTorrent protocol to download and distribute its Movie. This Court described the BitTorrent protocol in an earlier order in this case. *See TCYK, LLC v. Does 1–87*, 13 C 3845, 2013 WL 3465186 (N.D. Ill. July 10, 2013) (Dkt. 12). Other courts in this district have also explained how BitTorrent is used to download media. *See, e.g.*, *Malibu Media, LLC v. John Does 1–6*, 85 Fed. R. Serv. 3d 1187 (N.D. Ill. 2013); *Malibu Media, LLC v. Reynolds*, 12 C 6672, 2013 WL 870618 (N.D. Ill. Mar. 7, 2013).

To briefly summarize, BitTorrent is a software protocol that facilitates peer-to-peer file sharing used to distribute large data files over the Internet. An initial file-provider (the "seeder")

shares an initial file (the "seed") with a torrent network. Other users ("peers") intentionally connect to the seed file to download it. Each peer receives a segment (a "piece") of the file, then immediately becomes a source of that piece for other peers, relieving the seeder from having to send that piece in response to every new request. As additional peers request and receive pieces of the same file, each user becomes a part of the network from which the file can be downloaded. The group of seeders and peers uploading and downloading an identical file is called a "swarm." After a peer downloads the whole file, it continues to transmit pieces to other users until it disconnects, after which the pieces can continue to circulate throughout the swarm. The plaintiff alleges that each of the Doe defendants participated in the same BitTorrent swarm to download and distribute its Movie.

II. Motions to Quash and Motion for a Protective Order

In federal court, procedural issues involving subpoenas are governed by Federal Rule of Civil Procedure 45. Rule 45(a) allows the issuance of subpoenas to command a recipient to produce documents in one's "possession, custody, or control." Courts must quash a subpoena that (1) fails to allow a reasonable time for compliance, (2) requires a nonparty to travel more than 100 miles, (3) "requires disclosure of privileged or other protected matter, if no exception or waiver applies," or (4) "subjects a person to undue burden." Fed. R. Civ. P. 45(c)(3)(A). When assessing whether a subpoena subjects a person to undue burden, it considers whether the "burden of compliance with it would exceed the benefit of production of the material sought." *Nw. Mem'l Hosp. v. Ashcroft*, 362 F.3d 923, 927 (7th Cir. 2004). The party moving to quash bears the burden of showing that the subpoena falls into one of these impermissible categories. *Pac. Century Int'l, Ltd. v. Does 1–37*, 282 F.R.D. 189, 193 (N.D. Ill. 2012) (citing *Williams v. Blagojevich*, No. 05 C 4673, 2008 WL 68680, at *3 (N.D. Ill. Jan. 2, 2008)).

Here, three defendants move to quash the subpoenas that TCYK, LLC, has issued to their ISP. As a general rule, for a person to have standing to quash a subpoena issued to a nonparty, that subpoena must implicate that person's "legitimate interests." *See United States v. Raineri*, 670 F.2d 702, 712 (7th Cir. 1982). Courts in this district disagree on whether an anonymous defendant to a copyright infringement suit has standing to quash a subpoena issued to his or her ISP. *See reFX Audio Software, Inc. v. Does 1–111*, 13 C 1795, 2013 WL 3867656, at *1 (N.D. Ill. July 23, 2013). This Court concludes that the defendants have at least a minimal privacy interest in the information requested by the subpoena, which includes their telephone numbers, email addresses, and Media Access Control (MAC) addresses. *See Sunlust Pictures, LLC v. Does 1–75*, 12 C 1546, 2012 WL 3717768 (N.D. Ill. Aug. 27, 2012); *Third Degree Films, Inc. v. Does 1–108*, No. 11–3007, 2012 WL 669055, at *2 (D. Md. Feb. 28, 2012). Accordingly, the Court is satisfied that they have standing.

One defendant argues that the subpoenas violate "Supreme Court Rule 224." The Court understands this as a reference to Illinois Supreme Court Rule 224, which governs pre-suit discovery subpoenas used in Illinois trial courts to help plaintiffs identify responsible persons and entities. The defendant's reliance on this rule is misplaced. Rule 224 is merely "a tool for a party to use to obtain information as a precursor to the filing of a civil action" in an Illinois state trial court. *Alemayehu v. Boeing Co.*, 10 C 3147, 2010 WL 3328278 (N.D. Ill. Aug. 18, 2010). Rule 224 procedures "have no applicability in federal court." *Bond v. Wright Med. Tech., Inc.*, 12-CV-597-DRH-DGW, 2012 WL 2413051 (S.D. Ill. June 26, 2012). As the Court has explained, subpoena practice in federal court is governed by the Federal Rules of Civil Procedure. The Illinois Supreme Court Rules provide no basis for quashing the subpoenas here.

That defendant also argues that compliance with the subpoena would violate the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2702(a)(1). Section 2702(a)(1) of ECPA provides that "a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service." The defendant's invocation of § 2702(a)(1) is erroneous in this context, as other courts have explained. *See First Time Videos, LLC v. Does 1–500*, 276 F.R.D. 241, 247–48 (N.D. Ill. 2011); *Patrick Collins, Inc. v. Does 1–11*, 11-CV-01776-AW, 2011 WL 5439045 (D. Md. Nov. 8, 2011). The subpoenas contested here do not seek the contents of communications, such as the emails at issue in the case the defendant cites, *In re Subpoena Duces Tecum to AOL, LLC*, 550 F. Supp. 2d 606, 612 (E.D. Va. 2008). Instead, these subpoenas seek the names, addresses, telephone numbers, email addresses, and MAC addresses of the subscribers associated with the IP addresses known to the plaintiff—information pertaining to customer records, not the contents of communications. ECPA restricts the disclosure of customer records in 18 U.S.C. § 2702(a)(3). Yet ECPA also provides an exception under which an ISP "may divulge a record or other information pertaining to a subscriber or other customer . . . to any person other than a government entity." 18 U.S.C. § 2702(c)(6). Thus, ECPA allows the disclosure of this type of customer information to non-government entities, such as the plaintiff in this case. The ECPA challenge to the subpoena therefore fails.

Another defendant argues that the subpoena is overbroad and will not lead to relevant or admissible information. The Court is not convinced. Federal Rule of Civil Procedure 26(b)(1) allows parties to "obtain discovery regarding any nonprivileged matter that is relevant to the claim or defense of any party—including the . . . identity and location of persons who know of any discoverable matter." The Rules do not require information sought to be admissible so long

as it "appears reasonably calculated to lead to the discovery of admissible information." Fed. R. Civ. Pro. 26(b)(1). Another court in this district explained in a similar context:

> It is not a wild assumption on Plaintiff's part that the subscriber may be the alleged infringer or may lead to the alleged infringer. Without connecting the IP address to a person, Plaintiff would have no way of prosecuting infringement of its claimed copyright. The Court will not prohibit this discovery because it is less than certain to identify the individual who Plaintiff really wants to find.

Malibu Media, LLC v. John Does 1–49, 12-CV-6676, 2013 WL 4501443, at *2 (N.D. Ill. Aug. 22, 2013); *see also Zambezia Film Pty, Ltd. v. Does 1-65*, 13 C 1321, 2013 WL 4600385, at *3 (N.D. Ill. Aug. 29, 2013); *reFX Audio Software, Inc. v. Does 1–111*, No. 13 C 1795, 2013 WL 3867656, at *2 (N.D. Ill. July 23, 2013). The fact that the customer identified by the ISP in response to this subpoena may not be the infringer does not make the customer's identity irrelevant. The customer's identity may be a "useful starting point for identifying the actual infringer." *Malibu Media, LLC v. John Does 1–6*, 85 Fed. R. Serv. 3d 1187. The subpoena is calculated to lead to the identification of the infringer and will not be quashed just because the customer identified might eventually succeed in defending against the plaintiff's claim.

The defendant also argues that because the basis of the request has not been sufficiently verified, it would violate the defendants' due process rights to be subject to discovery without first being served with a complaint. Federal Rule of Civil Procedure 26(d) prohibits parties from seeking discovery "from any source" before the parties have conferred in accordance with Rule 26(f), except when authorized by the Federal Rules of Civil Procedure, stipulation, or a court order. District courts have broad discretion to manage the discovery process. *See James v. Hyatt Regency Chicago*, 707 F.3d 775, 784 (7th Cir. 2013). Courts "evaluate a motion for expedited discovery 'on the entirety of the record to date and the reasonableness of the request in light of all the surrounding circumstances.'" *Ibarra v. City of Chicago*, 816 F. Supp. 2d 541, 554 (N.D.

Ill. 2011) (quoting *Merrill Lynch, Pierce, Fenner & Smith, Inc. v. O'Connor*, 194 F.R.D. 618, 624 (N.D. Ill. 2000)). "For good cause, the court may order discovery of any matter relevant to the subject matter involved in the action." Fed. R. Civ. Pro. 26(b)(1). Good cause exists here because the plaintiff is unable to proceed without expedited discovery because it has no other way of identifying the defendants. *See TCYK, LLC v. Does 1–87*, 2013 WL 3465186, at *2. To the extent that the defendant attacks the reliability or accuracy of the plaintiff's method of identifying the putative defendants' IP addresses, it may mount such challenges in the course of its defense. *See Digital Sin, Inc. v. Does 1–176*, 279 F.R.D. 239, 242 (S.D.N.Y. 2012) (noting that the true offender is often not the name listed on the ISP account). To the extent that the defendant might be suggesting that the subpoena imposes an undue burden, the argument fails. The undue burden referred to by Rule 45 is the burden on the subpoenaed party. *See Malibu Media, LLC v. John Does 1–49*, 2013 WL 4501443, at *2 (citing *Malibu Media, LLC v. John Does 1–6*, 85 Fed. R. Serv. 3d 1187); *Malibu Media, LLC v. Reynolds*, 2013 WL 870618, at *6. Here, any burden of answering the subpoena falls on the ISP, not the defendants. These arguments each having failed, the motions to quash are denied.

One defendant also seeks a protective order, claiming generally that his or her privacy interests would be violated if the ISP provided the requested information to the plaintiff. The Court notes that should the plaintiff wish to name this defendant in an amended complaint, it will be constrained, as is every attorney who practices in this Court, by Rule 11(b), which states that an attorney submitting a filing to the court certifies that it is not "presented for any improper purpose, such as to harass" and that "the factual contentions have evidentiary support." Fed. R. Civ. P. 11(b). Naming a defendant in violation of those certifications could subject the plaintiff to sanctions. Fed. R. Civ. P. 11(c); *see also Hard Drive Prods. v. Does 1–48*, 11 CV 9062, 2012

WL 2196038, at *6 (N.D. Ill. June 14, 2012). To further protect the defendants against potential embarrassment or error in this case, this Court previously barred the plaintiff from publishing their identities in any way without leave of the court. *See TCYK, LLC v. Does 1–87*, 2013 WL 3465186. If individual defendants are later named in an amended complaint, they may then move to protect against the disclosure of their identities as appropriate. *See, e.g.*, *Malibu Media, LLC v. Reynolds*, 2013 WL 870618, at *7. The concerns the defendant expresses about harassment are purely hypothetical at this juncture. Should the plaintiff harass the Doe defendants after it obtains their contact information, the Court will consider their complaints and determine the appropriate remedies at that time. Without further information to shows why the protections already in place are insufficient to protect the defendants here, the request for a protective order is denied.

III. Motion to Sever

One defendant argues that the defendants in this case are improperly joined and requests that Does 2 through 87 be severed and dismissed from the case. Federal Rule of Civil Procedure 20(a)(2) permits people to be joined "in one action as defendants if: (A) any right to relief is asserted against them jointly, severally, or in the alternative with respect to or arising out of the same transaction, occurrence, or series of transactions or occurrences; and (B) any question of law or fact common to all defendants will arise in the action." Where the permissive joinder requirements are not met, Rule 21 gives courts the discretion to add or drop a party, or sever any claim against a party.

This Court has previously acknowledged that "[t]here is a split of authority nationally and within this district over whether it is appropriate to join in a single lawsuit many anonymous defendants who are alleged to have participated in a single BitTorrent swarm." *TCYK, LLC v. Does 1–87*, 2013 WL 3465186, at *3 (collecting cases); *Sunlust Pictures, LLC v. Does 1–75*,

2012 WL 3717768, at *3 (same). Substantial arguments exist on both sides of the split, but the Court is persuaded that joinder is appropriate here. The way that the BitTorrent protocol operates separates this case from the RIAA cases cited by the defendant. Even critics of mass joinder in copyright lawsuits acknowledge, "BitTorrent makes file sharing a cooperative endeavor." Sean B. Karunaratne, *The Case Against Combating Bittorrent Piracy Through Mass John Doe Copyright Infringement Lawsuits*, 111 Mich. L. Rev. 283, 290 (2012). "When the Doe defendants allegedly joined the swarm, they consented (implicitly, at least) both to download pieces of the Movie from other members of the swarm *and* to upload pieces of the Movie to other swarm participants." *TCYK, LLC v. Does 1–87*, 2013 WL 3465186, at *3.

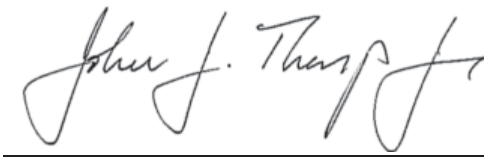
The complaint here alleges that each defendant "reproduced, distributed and offered to distribute [the Movie] among other [d]efendants" and that all defendants participated in "the same swarm," reproducing "the same seed file." Compl. ¶¶ 5, 14–15, Dkt. 1. The plaintiff characterizes the defendants' behavior as "collective and interdependent." *Id.* ¶ 14. The defendants allegedly participated in a swarm between May 1, 2013, and May 17, 2013. *See* Compl. Ex. B, Dkt. 1-1. To the extent that temporal proximity supports joinder, courts have held that a group of defendants who participated in the same swarm over comparable lengths of time may be joined. *See, e.g.*, *Pac. Century Int'l v. Does 1–31*, 11 C 9064, 2012 WL 2129003, at *2 (N.D. Ill. June 12, 2012) (joining defendants who allegedly participated in the same swarm for over one month). In light of these allegations, the claims against the defendants here arise from the same transaction or occurrence for the purposes of Rule 20(a), and the defendant is mistaken to argue that the plaintiff fails to allege that the defendants downloaded the file from one another.

This case also satisfies the second requirement for permissive joinder by involving common questions of law and fact for all defendants. Here, those questions include whether the

plaintiff is the copyright holder, whether copying that violates the Copyright Act has occurred, and whether participating in a BitTorrent swarm constitutes willful copyright infringement. *See Malibu Media, LLC v. John Does 1–6*, 85 Fed. R. Serv. 3d 1187; *Pac. Century Int'l v. Does 1–31*, 2012 WL 2129003, at *3; *First Time Videos, LLC v. Does 1–76*, 276 F.R.D. 254, 257–58 (N.D. Ill. 2011). The motion to sever is therefore denied. This does not foreclose future motions to sever. If individual defenses later overwhelm the case, or the Doe defendants are able to show that proceeding together will be inefficient or cause undue delay, the court retains broad discretion under Rule 21 to sever such parties and proceed separately at that time. *See Malibu Media, LLC v. John Does 1–6*, 85 Fed. R. Serv. 3d 1187.

* * *

For the reasons set forth above, the motions to quash the subpoenas, sever and dismiss the defendants, and impose a protective order are denied.



Date: October 9, 2013

John J. Tharp, Jr.
United States District Judge